CLAIMS

1. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

generating a first challenge signal of minimum duration T, where T is a fixed time interval;

generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

receiving a second ciphertext from said remote party, sending g^x modulo p to said remote party, and starting a clock;

receiving a third ciphertext and g^y modulo p from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

deriving a key k_B from g^y modulo p, computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, decrypting said second ciphertext with k_B to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

verifying that said second challenge signal is produced by said remote party;

producing a second response signal of minimum duration T, encrypting said second response signal with k_{AB} and sending a fourth ciphertext to said remote party;

verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with said remote party.

2. The method according to claim 1, wherein T is larger than the channel transmission and processing delay.

3. The method according to claim 1, wherein said challenge signals and response signals represent biometrics characteristics of the producing parties.

4. The method according to claim 3, wherein said biometrics characteristics include the voice of a person.

5. The method according to claim 1 ~~or 3~~, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

6. The method according to claim 1, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

7. The method according to claim 1, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

8. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

means for receiving a second ciphertext from said remote party, sending g^x modulo p to said remote party, and starting a clock;

means for receiving a third ciphertext and g^y modulo p from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

means for deriving a key k_B from g^y modulo p, computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, decrypting said second ciphertext with k_B to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

means for verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

means for verifying that said second challenge signal is produced by said remote party;

means for producing a second response signal of minimum duration T, encrypting said second response signal with k_{AB} and sending a fourth ciphertext to said remote party;

means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

9. The apparatus according to claim 8, wherein T is larger than the channel transmission and processing delay.

10. The apparatus according to claim 8, wherein said challenge signals and response signals represent biometrics characteristics of the producing parties.

11. The apparatus according to claim 10, wherein said biometrics characteristics include the voice of a person.

12. The apparatus according to claim 8 ~~or 10~~, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

13. The apparatus according to claim 8, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

14. The apparatus according to claim 8, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

15. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

computer readable program code means for generating a first challenge signal of minimum duration T, where T is a fixed time interval;

computer readable program code means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

computer readable program code means for receiving a second ciphertext from said remote party, sending g^x modulo p to said remote party, and starting a clock;

computer readable program code means for receiving a third ciphertext and g^y modulo p from said remote party, stopping the clock, and computing an elapsed time interval of said clock;

computer readable program code means for deriving a key k_B from g^y modulo p, computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, decrypting said second ciphertext with k_B to recover a second challenge signal from said remote party, decrypting said third ciphertext to recover a first response signal from said remote party;

computer readable program code means for verifying that said elapsed time of the clock is within a predetermined interval (TL_A, TU_A), where TL_A and TU_A are positive numbers;

computer readable program code means for verifying that said second challenge signal is produced by said remote party;

computer readable program code means for producing a second response signal of minimum duration T, encrypting said second response signal with k_{AB} and sending a fourth ciphertext to said remote party;

computer readable program code means for verifying that said first response signal is a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

16. The computer program product according to claim 15, wherein T is larger than the channel transmission and processing delay.

17. The computer program product according to claim 15, wherein said challenge signals and response signals represent biometrics characteristics of the producing parties.

18. The computer program product according to claim 17, wherein said biometrics characteristics include the voice of a person.

19. The computer program product according to claim 15 ~~or 17~~, wherein verification of said first response signal and said second challenge signal from said remote party is based on familiarity of remote party's biometrics characteristics.

20. The computer program product according to claim 15, wherein encryption of said challenge and response signals is performed using a cryptographic commitment function.

21. The computer program product according to claim 15, where TL_A is $t_1 + t_2$ and TU_A is $t_1 + t_2 + T$, with t_1 being the duration of said first challenge signal and t_2 being the duration of said first response signal.

22. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

receiving a first ciphertext from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

producing a first challenge signal of a minimum duration T, where T is a fixed time interval;

deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

receiving g^x modulo p from said remote party, deriving a key k_A from and g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from said remote party;

verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal, sending a third ciphertext and g^y modulo p to said remote party, and starting a clock;

receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with the remote party.

23. The method according to claim 22, wherein T is larger than the channel transmission and processing delay

24. The method according to claim 22, wherein said challenge signals and response signals are signals representing biometrics characteristics.

25. The method according to claim 22, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

26. The method according to claim 22, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

27. The method according to claim 22, wherein TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the first challenge signal and t_4 being the duration of the second response signal.

28. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

means for receiving a first ciphertext from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

means for producing a first challenge signal of a minimum duration T, where T is a fixed time interval;

means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

means for receiving g^x modulo p from said remote party, deriving a key k_A from and g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from said remote party;

means for verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal, sending a third ciphertext and g^{y} modulo p to said remote party, and starting a clock;

means for receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

29. The apparatus according to claim 28, wherein T is larger than the channel transmission and processing delay

30. The apparatus according to claim 28, wherein said challenge signals and response signals are signals representing biometrics characteristics.

31. The apparatus according to claim 28, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

32. The apparatus according to claim 28, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

33. The apparatus according to claim 28, wherein TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the first challenge signal and t_4 being the duration of the second response signal.

34. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

computer readable program code means for receiving a first ciphertext from said remote party, generating a random number y, computing g^y modulo p, where g and p are numbers;

computer readable program code means for producing a first challenge signal of a minimum duration T, where T is a fixed time interval;

computer readable program code means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext to said remote party;

computer readable program code means for receiving g^x modulo p from said remote party, deriving a key k_A from and g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from said remote party;

computer readable program code means for verifying that said second challenge signal is produced by said remote party, producing a first response signal of said minimum duration T;

computer readable program code means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal, sending a third ciphertext and g^y modulo p to said remote party, and starting a clock;

computer readable program code means for receiving a fourth ciphertext, stopping said clock, computing the elapsed time of the clock, and decrypting the fourth ciphertext to recover a second response signal from said remote party;

computer readable program code means for verifying that said elapsed time of said clock is within a predetermined interval (TL_B, TU_B), where TL_B and TU_B are positive numbers;

computer readable program code means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

35. The computer program product according to claim 34, wherein T is larger than the channel transmission and processing delay

36. The computer program product according to claim 34, wherein said challenge signals and response signals are signals representing biometrics characteristics.

37. The computer program product according to claim 34, wherein verification of said second challenge signal and said second response signal from remote party is based on familiarity with a remote party's biometrics characteristics.

38. The computer program product according to claim 34, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

39. The computer program product according to claim 34, wherein TL_B is $t_3 + t_4$ and TU_B is $t_3 + t_4 + T$, with t_3 being the duration of the first challenge signal and t_4 being the duration of the second response signal.

40. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

generating a first challenge signal of minimum duration T, where T is a fixed time interval;

generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

receiving g^y modulo p, computing a key k_B from g^y modulo p, decrypting the second ciphertext to recover a second challenge signal from said remote party;

verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with said remote party.

41. The method according to claim 40, wherein T is larger than the channel transmission and processing delay

42. The method according to claim 40, wherein said challenge signals and response signals are signals representing biometrics characteristics.

43. The method according to claims 40, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

44. The method according to claim 40, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

45. The method according to claim 40, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said second response signal.

46. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus including:

means for generating a first challenge signal of minimum duration T, where T is a fixed time interval;

means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

means for receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

means for receiving g^y modulo p, computing a key k_B from g^y modulo p, decrypting the second ciphertext to recover a second challenge signal from said remote party;

means for verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

47. The apparatus according to claim 46, wherein T is larger than the channel transmission and processing delay

48. The apparatus according to claim 46, wherein said challenge signals and response signals are signals representing biometrics characteristics.

49. The apparatus according to claims 46, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

50. The apparatus according to claim 46, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

51. The apparatus according to claim 46, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said second response signal.

52. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product including:

computer readable program code means for generating a first challenge signal of minimum duration T, where T is a fixed time interval;

computer readable program code means for generating a random number x, computing g^x modulo p, where g and p are numbers, deriving a key k_A from g^x modulo p, encrypting said first challenge signal with k_A and a symmetric key cryptosystem, and sending a first ciphertext to said remote party;

computer readable program code means for receiving a second ciphertext, sending g^x modulo p to said remote party, and starting a clock;

computer readable program code means for receiving g^y modulo p, computing a key k_B from g^y modulo p, decrypting the second ciphertext to recover a second challenge signal from said remote party;

computer readable program code means for verifying said second challenge statement to ensure that said second challenge statement is produced by said remote party, and producing a first response signal of minimum duration T;

computer readable program code means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

computer readable program code means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting the fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

computer readable program code means for verifying that said elapsed time of said clock is within a predetermined interval (tl_A, tu_A), where tl_A and tu_A are positive numbers;

computer readable program code means for verifying that said second response signal is a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key k from g^{xy} modulo p for secure communications with said remote party.

53. The computer program product according to claim 52, wherein T is larger than the channel transmission and processing delay

54. The computer program product according to claim 52, wherein said challenge signals and response signals are signals representing biometrics characteristics.

55. The computer program product according to claims 52, wherein verification of said second response signal and said second challenge signal from remote party is based on familiarity of remote party's biometrics characteristics.

56. The computer program product according to claim 52, wherein encryption of said challenge and response signals is carried out by a cryptographic commitment function.

57. The computer program product according to claim 52, where tl_A is $T_1 + T_2$ and tu_A is $T_1 + T_2 + T$, with T_1 being the duration of said first challenge signal and T_2 being the duration of said second response signal.

58. A method of authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said method including the steps of:

receiving a first ciphertext from remote party, generating a random number y, and computing g^y modulo p, where g and p are numbers;

producing a first challenge signal of minimum duration T, where T is a fixed time interval;

deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext;

receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from remote party, sending g^y to remote party and starting a clock;

verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration T;

computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

receiving a fourth ciphertext from said remote party, stopping said clock, decrypting said fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

verifying that said elapsed time of the clock is within an interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

verifying that said second response signal a response produced by said remote party to said first challenge signal; and

generating a key k from g^{xy} modulo p for secure communications with the remote party.

59. The method according to claim 58, wherein T is larger than the channel transmission and processing delay

60. The method according to claim 58, wherein said challenge signals and response signals are signals representing biometrics characteristics.

61. The method according to claim 58, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity of said remote party's biometrics characteristics.

62. The method according to claim 58, wherein encryption of challenge and response signals are carried out by a cryptographic commitment function.

63. The method according to claim 58, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said first challenge signal and T_4 being said duration of said second response signal.

64. An apparatus for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said apparatus:

means for receiving a first ciphertext from remote party, generating a random number y, and computing g^y modulo p, where g and p are numbers;

means for producing a first challenge signal of minimum duration T, where T is a fixed time interval;

means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext;

means for receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from remote party, sending g^y to remote party and starting a clock;

means for verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration T;

means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting said fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

means for verifying that said elapsed time of the clock is within an interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

means for verifying that said second response signal a response produced by said remote party to said first challenge signal; and

means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

65. The apparatus according to claim 64, wherein T is larger than the channel transmission and processing delay

66. The apparatus according to claim 64, wherein said challenge signals and response signals are signals representing biometrics characteristics.

67. The apparatus according to claim 64, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity of said remote party's biometrics characteristics.

67. The apparatus according to claim 64, wherein encryption of challenge and response signals are carried out by a cryptographic commitment function.

68. The apparatus according to claim 64, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said first challenge signal and T_4 being said duration of said second response signal.

69. A computer program product having a computer usable medium having a computer readable program code means embodied therein for authenticating a remote party and establishing a cryptographic key for secure communications via an insecure communications channel, said computer program product:

computer readable program code means for receiving a first ciphertext from remote party, generating a random number y, and computing g^y modulo p, where g and p are numbers;

computer readable program code means for producing a first challenge signal of minimum duration T, where T is a fixed time interval;

computer readable program code means for deriving a key k_B from g^y modulo p, encrypting said first challenge signal with k_B and a symmetric key cryptosystem, and sending a second ciphertext;

computer readable program code means for receiving g^x modulo p, computing a key k_A from g^x modulo p, decrypting said first ciphertext to recover a second challenge signal from remote party, sending g^y to remote party and starting a clock;

computer readable program code means for verifying said second challenge statement to make sure that said second challenge statement is produced by said remote party, and then producing a first response signal of minimum duration T;

computer readable program code means for computing g^{xy} modulo p, deriving a key k_{AB} from g^{xy} modulo p, encrypting said first response signal and sending a third ciphertext to said remote party;

computer readable program code means for receiving a fourth ciphertext from said remote party, stopping said clock, decrypting said fourth ciphertext with k_{AB} to recover a second response signal from said remote party;

computer readable program code means for verifying that said elapsed time of the clock is within an interval (tl_B, tu_B), where tl_B and tu_B are positive numbers;

computer readable program code means for verifying that said second response signal a response produced by said remote party to said first challenge signal; and

computer readable program code means for generating a key k from g^{xy} modulo p for secure communications with the remote party.

70. The computer program product according to claim 69, wherein T is larger than the channel transmission and processing delay

71. The computer program product according to claim 69, wherein said challenge signals and response signals are signals representing biometrics characteristics.

72. The computer program product according to claim 69, wherein verification of said second challenge signal and said second response signal from said remote party is based on familiarity with said remote party's biometrics characteristics.

73. The computer program product according to claim 69, wherein encryption of challenge and response signals are carried out by a cryptographic commitment function.

74. The computer program product according to claim 69, where tl_B is $T_3 + T_4$ and tu_B is $T_3 + T_4 + T$, with T_3 being the duration of said first challenge signal and T_4 being said duration of said second response signal.